Context-aware access control and anonymous authentication in WBAN

Amel Arfaoui, Omar Rafik Merad Boudia, Ali Kribeche, Sidi-Mohammed Senouci, Mohamed Hamdi

Context-aware access control and anonymous authentication in WBAN

Amel Arfaoui [a, *], *Omar Rafik Merad Boudia* [b], *Ali Kribeche* [a], *Sidi-Mohammed Senouci* [a], *Mohamed Hamdi* [c]

[a] *DRIVE EA 1859, University Bourgogne-Franche-Comté, France*
[b] *Computer Science Department, University of Oran 1 Ahmed Ben Bella, Algeria*
[c] *Digital Security Unit, Sup'Com University of Carthage, Tunisia*

The emergence of the Internet of Things (IoT) as the next generation megatrend has paved the way for pervasive, ubiquitous and proficient healthcare monitoring systems. In the di- verse kinds of networks, Wireless Body Area Network (WBAN) has been perceived as one of the most promising wireless sensor technologies for improving healthcare services thanks to its potential for continuous and real-time monitoring of health conditions. However, the open nature of wireless communication introduces wide security and privacy concerns as personal health information could be exposed to unauthorized parties or even malicious adversaries. Furthermore, in such a dynamic and heterogeneous environment where the context conditions continuously and frequently change, adaptive and context-aware solu- tions become mandatory to satisfy burgeoning security and privacy requirements. There- fore, it is indispensable to adaptively secure the extra-body communication between the smart portable device held by the WBAN client and the healthcare providers while consid- ering the dynamic context changes. In this paper, we propose a context-aware access control and anonymous authentication approach based on a secure and efficient Hybrid Certificate- less Signcryption (H-CLSC) scheme. Particularly, it incorporates the merits of Ciphertext-Policy Attribute-Based Signcryption (CP-ABSC) and Identity-Based Broadcast Signcryption (IBBSC) in order to meet the security requirements and provide adaptive contextual privacy. From a security perspective, the proposed mechanism achieves confidentiality, integrity, anonymity, context-aware privacy, key escrow resistance, public verifiability, and cipher- text authenticity. Performance analysis proves the efficiency and the effectiveness of the H-CLSC scheme compared to benchmark schemes in terms of functional security, storage, communication, and computational cost.

1. Introduction

In recent years, the rapid technological advancements in wireless communication and the melding of innovations in the fields of ubiquitous sensing and pervasive computing have performed a significant role in the emerging Internet of Things (IoT) paradigm. In fact, IoT has tremendous potential to create value and provide appropriate solutions for a wide range of applications such as smart cities, security, visual sensing, image communication, and healthcare (Aziz and Pham, 2013; Pham and Aziz, 2013). Specifically, the IoT holds great promise

* Corresponding author.

for the healthcare area, where its features are already being exploited to improve the reliability of remote health monitoring systems (Zhibo, 2013). In remote patient monitoring systems, the personal health information (PHI) is collected by Wireless Body Area Network (WBAN) and aggregated by a data sink, such as Smartphone, tablet, or PDA. Then, the data is transmitted to the medical staff to assess the patient's status and provide the appropriate clinical diagnosis. In this context, it is critical to secure the transmitted data between the WBAN client and the remote application providers (APs) such as the hospital, physician or medical staff.

In fact, the collected data should be handled, transmitted, and analyzed only by authorized parties in order to ensure accurate diagnosis and treatments. Since the patient's information is transmitted through an open channel, it can be eavesdropped, intercepted and modified. Consequently, counterfeited health-related data may mislead the caregivers to make the appropriate decision, which may convolute the patient's situation. Furthermore, the dynamics of cellular networks imposes more challenges to design robust security and access control mechanisms. As to the security facet, one of the main issues is authentication and access control of patients' personal health information while considering the dynamic context changes to make the right decision at the right time by the right party. Therefore, it is necessary to define who can access what and under which contextual information. For this purpose, according to the information sensitivity, the data consumer role, as well as the patient's condition sensitivity, different access rights, and permissions can be assigned. For example, a nurse who has restricted access compared with a doctor in normal situations can gain additional permissions in emergency situations. In such a critical context, privacy may be restricted or relaxed given that safety is more important than security. Currently, security and privacy preservation of extra-body communication have attracted particular attention. However, most of the previous works mainly focus on either anonymous authentication or privacy preserving concerns while ignoring the dynamic context changes (Zhang et al., 2017; Rongxing et al., 2013; Chunqiang et al., 2016). On the one hand, they don't incorporate the contextual information related to the dynamic nature of cellular networks in the authentication and authorization decision. On the other hand, many proposed access control schemes suffer from the following problems: (i) they need public key certificates, they are exposed to the impersonation attack by the Key Generator Center (KGC) as well as key escrow problem (Chunqiang et al., 2016; junzuo et al.,2013; Xianping et al., 2016). (ii) They don't provide either ciphertext authenticity or public verification. In fact, the receiver should decrypt at first the ciphertext and then verify its validity which may waste the computation resources and increase the response delay if the ciphertext is not valid.

This study is devoted to investigating the cryptographic primitives to address the above issues. We notice that there are other equally serious security concerns in WBAN, such as the key management (Huawei et al., 2013, 2015) and the access policies management for sensor nodes (Kriangsiri et al.,2009; Tan et al., 2009) in the intra-body communications. However, the study of those issues is out of the scope of this paper.

1.1. *Contributions*

In this paper, we focus on extra-body communication. Specifically, we propose a novel approach for the design of a context-aware authentication and access control scheme to adaptively adjust the security and privacy level according to the contextual information. For this purpose, we use an efficient and secure Hybrid Certificateless Signcryption (H-CLSC) scheme with public verifiability and ciphertext authenticity that can simultaneously authenticate users and protect query messages. The proposed to address the secure communication problem and provide adaptive context-aware privacy. A WBAN client in a normal situation can control access to his own data. For example, by constructing the access structure ({status=normal} AND {hospital *A*} AND {Vascular Surgery}), the data requires that on normal situations only doctors from the Vascular Surgery Center in hospital *A* can have the access right. The novelties of our proposed model are summarized as follows.

- A novel context-aware authentication and access control approach that provides a dynamic authorization to the patient's data while considering the contextual information (patient's condition severity, data consumers' roles, security domain...).
- A Hybrid Certificateless Signcryption (H-CLSC) scheme with public verifiability and ciphertext authenticity in which the validity of the ciphertext can be verified without decryption.
- An anonymous signcryption mechanism to provide efficient and fine-grained encrypted access control by merging the worthiness of CP-ABSC and IBBSC. The WBAN client can control who has access to his personal health information by defining an access structure for data.
- Dealing with the key escrow problem and impersonation attack by the KGC. The data owner/consumer's private keys aren't generated by the KGC alone but by a combination of the contributions of the KGC and the data owner/consumer. Given that the KGC can generate only the user's partial private key, it cannot decrypt messages or impersonate users.

1.2. *Organization*

The remainder of this paper is organized as follows. Section 2 highlights some previous works related to security and privacy mechanisms in WBAN. A mathematical background is presented in Section 3. The system model and the design goals in terms of context-aware privacy and security requirements are described in Section 4. The efficient H-CLSC scheme for authentication and access control as well as its security model are given in Section 5, followed by the performance analysis in Section 6. Finally, Section 7 concludes the paper.

2. Related work

Security and privacy of a patient's health records are two crucial features for the system security of the WBAN. On the

one hand, security implies data is protected from unauthorized users when being, collected, transferred and stored. On the other hand, privacy means that the data can only be accessed and used by the authorized parties. It defines who can access what and under which context (Javadi and Razzaque et al., 2013). Therefore, it is essential to deal with the issues allied with security and privacy preservation in WBAN. Some contributions have proposed authentication and key agreement schemes for intra-WBAN communication (Huawei et al., 2013, 2015; Liu et al., 2015). Particularly, Huawei et al. (2013) discussed the key management problem in WBAN. They used a fuzzy commitment technology with a weak time synchronization mechanism and an energy-based multi-hop-route-choice method to implement efficient key management among sensor nodes. In addition, Huawei et al. (2015) exploited the biometric characteristics to implement an authentication scheme for WBAN. Specifically, they proposed two approaches: the first approach presents a new key negotiation scheme between body sensor nodes based on the fuzzy extractor technology. The second approach provides an improved linear interpolation encryption method for biometric data. Liu et al. (2015) developed two authenticated key exchange protocols for two-hop star WBAN topology, which grants selective authentication between the sensor nodes according to the application scenario. The first protocol is designed for the communication between the sensor nodes and the controller node in normal situations. The second protocol is applied in an emergency scenario where fast responses and communication between sensor nodes are needed.

Recently, some contributions have addressed particular attention to authentication and access control for extra-body communication. Particularly, the cryptography-based authentication scheme has been widely adopted and implemented using the traditional public key cryptography (TPKC) (Ming et al., 2010, 2013). In this scheme, a Certificate Authority (CA) is required to issue and maintain a pool of certificates for the clients after verifying their validity, which arises inevitably in the awkward certificate management problem. For this purpose, the elliptic curve cryptography (ECC) has been introduced as an alternative to providing the same security level with better performance and much smaller key size for environments with limited battery capacity and computing capabilities. Nevertheless, public key infrastructure (PKI) is needed in the practical implementation of the ECC. It employs a digital certificate to bind the user's identity to the public key. To mitigate the problem of certificates management, several identity-based (ID-based) authentication schemes (Zhang et al., 2017; Liu et al., 2014; He et al., 2016; Li et al., 2016; Liu et al., 2016; Hu and Qin, 2015) were proposed. In such a proposal, a user's public key is determined from its identity information, such as identity numbers and e-mail. For the private key, it is computed by a trusted third party named the Private Key Generator (PKG). Even if the lightweight identity-based cryptography is considered as a very suitable mechanism for resource-constrained WBANs, it suffers from the key escrow problem since the PKG generates all users' private keys.

To address the above problems and ensure secure extra-body communication in WBAN, Liu et al. (2014) used the bilinear pairing defined on the elliptic curve to design a new anonymous authentication scheme based on the certificateless signature. A user should be authenticated before access the patient's health information stored in the network server. The proposed model can avoid both public key certificates and key escrow problem because the key generation incorporates both the user and the KGC. However, the adoption of this scheme is restricted to users who access a network server, not the WBAN. In addition, He et al. (2016) found that the above scheme suffers from the impersonation attack. Therefore, they provided an improved anonymous authentication scheme to address the aforementioned security problem. In Li et al. (2016), the authors proposed an efficient certificateless signcryption model for access control in WBAN. In the registration phase, every user first generates a public key pair and sends it to the KGC in order to get a partial private key. Upon receiving his partial private key, the user could compute his full public key pair. As only registered users could generate this public key pair, this generation can be considered as a measure to verify the user legitimacy. Given that only the public key is transferred, the user's identity is hidden and anonymity is ensured. However, in their scheme, they don't consider the data consumer's role. Thus, all data consumers have the same access privileges. In Liu et al. (2016), a cost-effective anonymous authentication scheme that could protect the identity and privacy of the user was designed. In Zhang et al. (2017) an efficient and certificateless scheme based on the generalized signcryption (CLGSC) model was proposed. The security analysis illustrated the capacity of the adopted scheme in terms of data confidentiality and integrity, mutual authentication, unlinkability, anonymity, etc. From the performance perspective, it has been demonstrated that it can outperform the existing schemes in terms of computational and communication overhead. In Hu and Qin, (2015), a remote anonymous authentication protocol with revocability for extra-body communication in WBANs has been proposed. However, it involved large amounts of computation and energy consumption. In Jiankun et al. (2010), the authors presented a Hybrid Public Key Infrastructure (HPKI) that uses smart cards to provide a contract-oriented e-health security architecture. In the proposed scheme, trust and security management are delegated to the medical service provider during the contract period of the medical treatment. However, the HPKI model suffers from several attacks such as man-in-the-middle attack and replay attack. In addition, if a contract key is compromised, the trusted entity can still access the corresponding PHI data encrypted with the compromised key.

Attribute-Based Cryptography (ABC) is considered as a promising tool that can provide fine-grained and adaptive access control. Specifically, in Ciphertext-Policy Attribute-Based Encryption (CP-ABE), each user is associated with a set of attributes and the data is encrypted according to an access structure. Only receivers whose attributes satisfy the access policy can decrypt the ciphertext. In Lu et al. (2013), the authors proposed an opportunistic privacy preserving model in WBAN. They considered data processing techniques in emergency situations for M-Health systems with minimal privacy disclosure. A CP- ABE scheme was proposed in Hu et al. (2016) to secure data communications between the sensor nodes, data sink, and data consumers. In the proposed approach, role-based access control is adopted by employing an access control tree constructed from the data attributes. However,

such schemes suffer from the key escrow problem in which a curious KGC has the power to decrypt every ciphertext. Furthermore, most of the existing Attribute-Based Encryption (ABE) constructions depend on a single key authority which may open the door for potential privacy exposure. To remedy this weakness, several research works adopt multi-authority ABE as an attractive solution that can successfully avoid delegating trust to a single authority by making the system distributed. This model allows the sender to specify for each authority its monitored set of attributes. Nonetheless, it is burdensome for a user to prove his attributes to several key authorities and get his private key over a secure channel and it needs high computation cost.

Most of the aforementioned works don't involve the contextual information in their access control and authentication schemes. On the one side, they don't consider the severity of the patient's condition in the medical environment given that in some situations the safety should be prioritized and the privacy could be relaxed or restricted. On the other side, they don't differentiate between the personal and public domains, which have different attribute definitions, key management requirements, and scalability issues. In this context, the following critical technical challenges should be considered when designing a WBAN security mechanism: (i) How to properly regulate and adjust the access rights and authentication policy of the different data consumers while considering the dynamic context changes? (ii) How to guarantee that any third party can judge whether data is altered by attackers without access to the message? (iii) How to resolve the key escrow problem and mitigate the impersonation attack by the KGC? (iv) How to be lightweight for resource-constrained devices, i.e., low computational, storage and communication overhead? The context-aware access control and anonymous authentication approach proposed in this paper and detailed in the next sections deals with all these technical challenges.

3. Preliminaries

In this section, we briefly review the mathematical background of Bilinear Pairings and the cryptographic primitives used in this paper.

3.1. *Bilinear pairings*

Let $\mathbb{G}_1$ be a cyclic additive group of prime order q and $\mathbb{G}_2$ be a cyclic multiplicative group of the same order q. A bilinear pairing is a map e:$_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$ and satisfies the following properties:

- *Bilinear*: A map e: $\mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$ is bilinear if and only if $\forall P, Q \in \mathbb{G}_1$ and $a, b \in \mathbb{Z}_q$, we have $e(aP, bQ) = e(P, Q)^{ab}$
- *Non-degeneracy*: $\exists P, Q \in \mathbb{G}_1$ where $e(P, Q) \neq 1\mathbb{G}_2$
- *Computability*: $\forall P, Q \in \mathbb{G}_1$, there is an efficient algorithm to compute e (P, Q) in polynomial time.

The security of the proposed scheme depends on the following intractable problems:

- *Computational Diffie–Hellman(CDH) problem*: given $P, aP, bP \in \mathbb{G}_1$, $\forall a, b \in Z_q^*$, it is infeasible to compute abP in polynomial time. The advantage of any probabilistic polynomial time algorithm B in solving the CDH problem is defined as $Adv_B^{CDH} = \Pr[\mathcal{B}(P, aP, bP) = abP | a, b \in Z_q^*]$. The CDH Assumption requires that for any probabilistic polynomial time algorithm B, the advantage Adv_B^{CDH} is negligible.
- *DBDH (Decision Bilinear Diffie–Hellman) problem*: Given two groups $\mathbb{G}_1$ and $\mathbb{G}_2$ with the same prime order q, a bilinear map e: $\mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$, $T \in \mathbb{G}_2$ and a generator P of $\mathbb{G}_1$, the DBDH objective is to decide whether $T = e(P, P)^{abc}$ holds or not in $(\mathbb{G}_1, \mathbb{G}_2, e)$ from the given (P, aP, bP, cP), $\forall a, b, c \in Z_q^*$. We say that an algorithm B that generates $b \in \{0, 1\}$ has advantage ε in solving DBDH problem in $\mathbb{G}_1$ if:

$$\left| \Pr\left[\mathcal{B}\left(P, aP, bP, cP, e(P, P)^{abc}\right) = 0 \right] - \Pr[\mathrm{B}(P, aP, bP, cP, r) = 0] \geq \varepsilon \right|$$

Where the probability is over the random choice of $a, b, c \in Z_q^*$, the random choice of $r \in \mathbb{G}_2$ and the random bits of $\mathcal{B}$.

3.2. *CP-ABSC protocol description*

The CP-ABSC scheme includes the following four algorithms, namely, Setup, KeyGen, Signcryption and Designcryption.

- Setup (1^λ): Given a security parameter λ, the KGC generates a master secret key MK that is kept private and a public key PK shared by users.
- KeyGen (PK, MK, U): The KGC takes the master secret key MK, the attribute set of the user U, and the public key of the system PK as inputs. It generates the private key SK_U.
- Signcryption $(PK, M, SK_{Us}, \mathbb{A})$: The signer takes the public parameters PK, a plaintext M, a signing private key SK_{Us} and an access structure $\mathbb{A}$ as inputs. The algorithm will signcrypt M and generate a ciphertext CT such that only a user who possesses a set of attributes that satisfy the access policy will be able to designcrypt.
- Designcryption (CT, PK, SK_{Ud}): The receiver takes as input the ciphertext CT, the public parameters PK and his decryption key SK_{Ud}. The algorithm outputs a message M or a reject symbol $\perp$.

3.3. *IBBSC protocol description*

The IBBSC scheme consists of four algorithms, namely, Setup, KeyGen, Signcryption and Designcryption.

- Setup (1^λ): The KGC takes a security parameter λ as an input. Then, it outputs a master secret key MK and a public key PK.
- KeyGen (PK, MK, ID): The KGC takes the master secret key MK, the identity $ID \in \{0, 1\}^*$, and the public key of the system PK as inputs. It outputs the private key SK_{ID}.
- Signcryption (PK, M, S, SK_{IDs}): The signcryption algorithm is executed by the sender which takes the public parameters PK, the signing key $SK_{IDs,}$ a plaintext M, and a set of identities $S = \{ID_1, \ldots ID_n\}$ of receivers as inputs. It encrypts the plaintext M to generate the ciphertext CT.
- Designcryption (CT, PK, SK_{IDd}): The receiver takes as input the ciphertext CT, the public parameters PK and the

decryption key SK_{IDd}. The algorithm outputs a message M or a reject symbol $\perp$.

3.4. *Conversion between access structures DNF and a set of identities*

Attribute-Based Encryption (ABE) was introduced as an extension of the notion of Identity-Based Encryption (IBE) in which user identity is viewed as a set of expressive attributes instead of a single string defining the user identity (Herranz , 2017; Sahai and Waters, 2005). Compared with identity-based encryption, ABE is considered as a promising tool that provides one-to-many encryption and ensures a fine-grained access control. Besides fine-grained access control, privacy-preservation is considered as a critical concern to be handled. In fact, in some crucial situations, not only the data but also the access policy could be sensitive information. Specifically, the access policies may reveal sensitive data, such as the patient's identity, treatments or symptoms indicating the patient's status and diseases. In this vein, both patients and healthcare providers should remain hidden from unauthorized parties or adversaries. In addition, the adversary should be hampered from associating the transmitted personal health information to a patient. Although CP-ABSC provides a fine-grained access policy, it suffers from some problems: (i) the access policies attached to the ciphertext are public. Under such an assumption, unauthorized users can learn information about the underlying data itself. (ii) It brings out high communication overhead in data sharing given that the length of private keys increases linearly with the number of the attributes.

To overcome the above problems, we will combine the features of CP-ABSC and IBBSC to provide a constant-size of private keys, hidden access policy, certificateless signcryption, etc. In this context, we will exploit the conversion between an IBBSC and a CP-ABSC that supports Boolean functions in DNF (Fan et al., 2017; Herranz, 2017). For such a scheme, an access structure $\mathbb{A}$ which admits, at least, AND policies can be uniquely related to an identity $ID_{\mathbb{A}}$, whose length equals to $|U|$, i.e., the size of the universe U of attributes. Specifically, for an access structure $\mathbb{A}$, for $i = 1$ to $|U|$, if an attribute X_i is in $\mathbb{A}$, then set the ith bit of $ID_{\mathbb{A}}$, as 1; otherwise, set it as 0. For instance, if $U = \{A, B, C, D, E\}$ and $\mathbb{A} = A$ AND B OR C, then we can construct the identity as $ID_{\mathbb{A}} = \{11{,}000, 00100\}$. An access structure can be represented as a disjunction of conjunctive clauses, i.e. disjunctive normal form (DNF). In this context, a DNF structure implies a set of identities $S = \{ID_1, \ldots ID_n\}$, which can be considered as the receivers set in an IBBSC scheme.

As mentioned above, an access structure is considered as a set of attributes that corresponds to a set of identities. When the identity associated with the ciphertext satisfies the signing access structures, the data consumer can get the medical data. Fig. 1 shows an example of the access structure. For example, an access structure has the following attributes, i.e., Department: Vascular surgery, Position: Doctor, Location: hospital A, is uniquely assigned to an identity ID1. Hospital A indicates to which hospital the doctor associated. Vascular surgery specifies the doctor's department. If the identity of the data consumer satisfies the signing access structure, the doctor can access the patient's medical data and give treatments

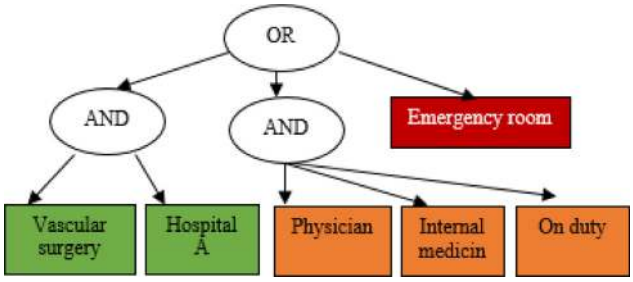

Fig. 1 – An example of access structure.

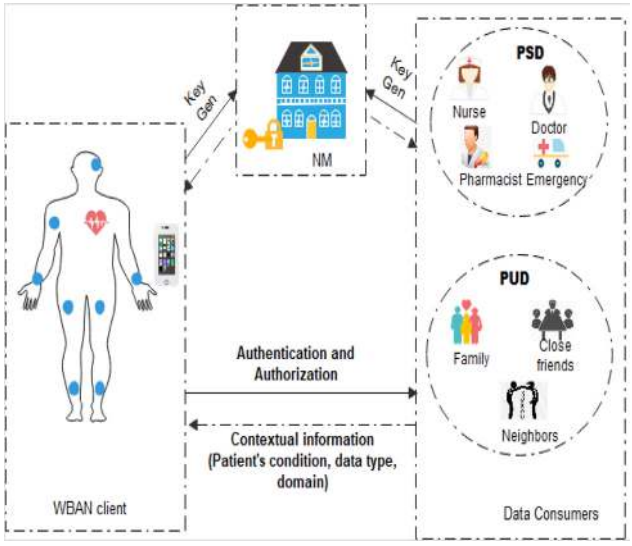

Fig. 2 – System model.

to the patient. The same is true for a physician on duty or the emergency room.

4. Models and design goals

In this section, we present the system model. Then we describe the threat model and the different security requirements. Finally, the contextual information that influences the access policy is defined.

4.1. *System model*

We consider a WBAN communication system presented in Fig. 2. It mainly consists of three entities: The Network Manager (NM), the WBAN client and the data consumers (such as a nurse, a doctor, an insurance company a physician, family member, close friend…). The different functions of each entity are presented as follows:

- NM is a powerful entity responsible for system initialization and participant's management. In addition, it is considered as a Key Generator Center (KGC) for the generation of public parameters and users' secret keys assignment. As the NM may be carried out by the healthcare provider's center or a commercial organization, it cannot

be fully trusted. Consequently, the NM only generates a partial private key for the user and it is prohibited to access the patient's health information. Therefore, we can mitigate the key escrow problem and the impersonation attack by the NM.

- WBAN Client consists of a set of sensor nodes and a controller which is used to store the patient's data in an encrypted form. When a data consumer wants to access to a data item from the WBAN client under given contextual information, he can verify the validity of the ciphertext and decrypt the data as long as he possesses the decryption attributes set specified by the signing access structure.
- Data consumers refer to users coming from two different domains, namely public domain (PUD) and personal domain (PSD) (Li et al., 2013). Data consumers in PUD include healthcare providers, e.g., doctors, physicians, nurses, and researchers. However, users who come from the PSD are personally related to the WBAN client (such as family members or close friends). To decrypt a message, data consumers need not only to have the attributes that satisfy the access structure specified by the data owner but also to determine the contextual information related to their domain, the patient's situation, and the data type in order to define their permissions.

4.2. *Threat model*

We consider the NM to be semi-trusted, i.e., curious but honest. That means it will try to disclose as much as possible the secret patient's health information, but it will honestly follow the exchanges between communicating parties. The NM may also impersonate the patient and data consumers. Furthermore, some data consumers will try to access to the WBAN client's data beyond their privileges. In addition, we are concerned with various types of adversaries that can launch different attacks on the system. On the one hand, an adversary may eavesdrop the communication channel, modify or inject counterfeit data during the transmission and reply previously delivered messages. For instance, the eavesdroppers may deduce the source's disease once they find the intended doctor of the WBAN client. Therefore, the privacy of the WBAN client and data consumers is required. On the other hand, it is possible for unauthorized or malicious data consumers to trace back the WBAN client's actions. In this context, it is also needed to guarantee the untraceability for the patient during the exchanges.

4.3. *Security requirements*

The dynamics of the cellular network and the wireless communication between the data owner and the data consumer make the authentication and the patient's privacy vulnerable to many attacks. To guarantee secure extra-body communication, a dynamic and context-aware authentication and authorization scheme should be conceived to ensure the following security and contextual privacy requirements. Based on the previous works (Li et al., 2016; Xiong, 2014; Samaneh et al., 2014) and the above analysis, the authentication and authorization scheme should satisfy the following functionality features and security requirements.

- *Ciphertext Authenticity and public verifiability*: To guarantee that only authorized data consumers could access the patient's health information and query messages be protected. It is essential to provide a ciphertext authenticity and public verifiability where the validity and the origin of the ciphertext can be verified without revealing the content of the message or the receiver's private key.
- *Context-aware privacy*: Based on the contextual information (the patient's condition severity, the data consumer's role, the data type, etc.), the authentication policy and the access structure are defined.
- *Anonymity*: To protect the patient's privacy, it is essential to ensure that no one including unauthorized data consumers and the NM could obtain the patient's identity from the intercepted message.
- *Non-traceability*: Only anonymity is insufficient for privacy preservation. Therefore, it is necessary that the authentication scheme could guarantee non-traceability, i.e., adversaries, unauthorized data consumers, and NM cannot trace the WBAN client's action.
- *Resilience against attacks*: Due to the dynamic and open structure of WBAN, the access control and authentication for WBAN are susceptible to many attacks such as unauthorized access, the impersonation attack, the replay attack, and the modification attack. Therefore, the authentication and authorization scheme should avoid those attacks.

4.4. *Patient's contextual information*

In a healthcare system, medical data should be collected only by the well authenticated and authorized parties when it's needed and depending on the dynamic context changes. In this context, the authentication and authorization policy is defined on the basis of the current situation of both the data owner and the data consumer. It considers not only the data consumer's credentials but also the contextual information which may include the patient's condition, the data sensitivity as well as the data consumers' domain.

4.4.1. *Patient's condition*

It is necessary to provide dynamic access control while considering the severity of the patient's condition. In fact, it may be classified as normal, serious or emergency reflecting the context that influences the decision-making and the access policy. For instance, in emergency situations, access to the requested data should be granted immediately. In such cases, access is admitted to the requested data regardless of the risk. In this context, each access right to the WBAN client's health information is also delegated to the emergency room. To prevent the abuse of access without privileges, the emergency staff should contact the NM that manages the emergency room to verify his identity and the emergency situation to obtain temporary access. After the emergency is over, the patient can revoke access via the emergency room. Concretely, a patient with vascular disease can encrypt his data and create the access structure to his own data in an emergency situation labeled as {"vascular disease; emergency"}. Therefore, he permits access to his medical history given that in such cases safety is more important than privacy. In addition, he sends

the emergency secret key to the NM through a secure channel. In the proposed model, privacy is relaxed in emergency situations by the fact that clinicians who don't have access to patient health information in normal situations can gain temporary access in critical situations. In fact, in such cases, data availability is more important than confidentiality and the patient may be unconscious, so, unable to change his access policies beforehand. Therefore, the NM will be alerted by the controller which informs the caregivers that a critical situation occurred. Then, the NM finds the medical staff and assigns their access privileges (emergency key) of the patient's medical data according to the emergency case in order to decrypt the stored data in an encrypted form.

4.4.2. *Data type*

The patient's health records consist of sensitive information such as disease details, family history, treatments, medications, and dosing. But other information such as healthy diet and physical exercise is considered as not sensitive. Therefore, the data should be classified into different categories on the basis of their sensitivity.

4.4.3. *Data consumer's domain*

In general, data consumers come from two different domains, namely public domain (PUD) and personal domain (PSD) (Li et al., 2013). The PUD includes users who make access based on their professional roles (doctors, nurses, physicians, medical researchers…). They should have access to the patient's sensitive data for diagnosis, treatments, and analysis. On the other side, in PSD, data users are personally associated with a data owner (family members, close friends…) and their access privileges are assigned on the basis of their relationship with the data owner. In order to make the right decision at the right time, they need to have the right information on time about the patient's condition (emergency situation, a disease, treatments…).

5. Efficient Hybrid Certificateless Signcryption (H-CLSC) scheme

In this section, we present the proposed H-CLSC scheme. Then, we give its security model. We exploit the transformation between CP-ABSC and IBBSC (Fan et al., 2017; Javier, 2017) which considers an access structure as a set of identities. As mentioned above, a set of attributes are *uniquely* related to identity. The signer who possesses his own signing key can sign a message if his signing attribute set (corresponding to an identity ID_s) satisfies the signing policy.

Based on the contextual information (patient's condition, the data sensitivity, data consumers' domain) and the set of decryption attributes (corresponding to an identity ID_d), only the data consumer whose attribute set verifies the access structure can decrypt the ciphertext (Pang et al.,2015; Li et al., 2016).

5.1. *H-CLSC algorithm*

In order to provide hidden access policy for privacy preservation, a constant size of private keys and mitigate the key escrow problem in CP-ABSC scheme, we introduce the construction concept of a CP-ABSC scheme from an IBBSC scheme. Based on this transformation, an access structure is viewed as a set of identities. In addition, a user can generate his *own* secret key that the NM cannot obtain because it generates only the partial private key. Assume that IBBSC is an identity-based broadcast signcryption scheme with the four phases: System Initialization, Key Generation, Signcryption, and Designcryption. We define the proposed Hybrid Certificateless Signcryption (H-CLSC) scheme as the construction of a CP-ABSC on the basis of IBBSC as follows.

- *System Initialization* (1^λ): This algorithm runs ($IBBSC.MK$, $IBBSC.PK$) $\leftarrow$ $IBBSC.Setup(1^\lambda)$ and generates the master key MK and the public key PK as $(MK, PK) = (IBBSC.MK, IBBSC.PK)$.
- *Key Generation* (PK, MK, U): This algorithm takes the public key PK, the master key MK and the set of attributes U as inputs and converts the set of attributes U to an identity $ID_U \in \{0, 1\}^{|U|}$. It outputs the private key $SK_U = IBBSC.SK_{IDU}$ as follows: $IBBSC.SK_{IDU} \leftarrow IBBSC.KeyGen(PK, MK, ID_U)$. In our scheme, we use two private keys for signing and decryption.
- *sExtract (PK, MK, U_s):* Given a set of signing attribute set U_s, a public key PK and master key MK as inputs, the algorithm generates the signing private key SK_{Us}.
- *dExtract (PK, MK, U_d, c):* Given a public key PK, a master key MK, a set of decryption attributes U_d and a contextual information c provided by the receiver, the algorithm outputs the decryption private key SK_{Ud}.
- *Signcryption* (PK, M, SK_{Us}, $\mathbb{A}$, c): The signcryption algorithm takes as inputs the public parameters PK, a plaintext M, the signer private key SK_{Us}, an access structure $\mathbb{A}$ which is converted to set of identities $S = \{ID_1, \ldots ID_n\}$ of receivers and a contextual information c. It outputs the ciphertext CT as follows: $IBBSC.CT \leftarrow IBBSC.signcryption(M, PK, S, SK_{IDs}, c)$.
- *Designcryption* (CT, PK, SK_{Ud}): The decryptor takes as input the ciphertext CT, the public parameters PK and the receiver's private key SK_{Ud}. The algorithm gets the plaintext M by executing $IBBSC.M \leftarrow IBBSC.Designcrypt(CT, PK, SK_{Ud})$.

5.2. *Security model of the proposed H-CLSC scheme*

In this subsection, we formally define the security of the proposed scheme against chosen plaintext attacks. We will use the following games in Section 6 to prove the security of the proposed scheme.

Confidentiality: The proposed H-CLSC scheme is said to be indistinguishable against chosen ciphertext attacks (IND-(H-CLSC)-CCA) if no PPT adversary A has a non-negligible advantage in winning the following game with a challenger B.

Setup: The challenger B performs the Setup(1^λ) algorithm of the H-CLSC scheme, sends the public key PK to the adversary A and keeps the master secret key MK to itself. After receiving the public parameters, the adversary declares the set of identities (corresponding to a DNF challenge access structure A^*) $S^* = \{ID_1{}^*, \ldots ID_n{}^*\}$.

Query Phase 1: The adversary A can ask a polynomial bounded number of queries in an adaptive manner as follows:

- sExtract query: In this query, the adversary can adaptively ask for the signing secret key of the attribute set U_s. For the set of the signer attributes, the challenger *B* executes *sExtract* (*PK*, *MK*, U_s) → SK_{Us} and sends SK_{Us} to the adversary.
- dExtract query: In this phase, the adversary can adaptively ask for decryption secret keys for the sets of attributes U_{d1}…, U_{dn} which are converted to a set of receivers' identities $S = \{ID_1, \ldots ID_n\}$ under a contextual information *c*. For each U_{di}, the challenger runs *dExtract* (*PK*, *MK*, U_{di}, *c*) → SK_{Udi} and sends SK_{Udi} to the adversary. The restriction is that none of the queried set should satisfy the challenge access structure, i.e., ∀i ∈ [n]: $ID_i \neq ID_i{}^*$.
- Signcryption query: The Adversary *A* executes the Signcryption algorithm to get the ciphertext *CT* = *Signcryption* (*PK*, *M*, SK_{Us}, 𝔸, *c*), it takes as input the public key *PK*, the plaintext *M*, the signer private key SK_{Us}, the access structure 𝔸 which is converted to a set of receiver's identities *S* = $\{ID_1, \ldots ID_n\}$ and a contextual information *c*.
- Designcryption query: The adversary issues decryption queries and sends to *B* (*CT**, ID_i) where *CT** is the ciphertext generated by *A* and ID_i is the identity chosen by *B* and ID_i ∈ *S**. *S**= $\{ID_1{}^*, \ldots ID_n{}^*\}$ is the set of identities (corresponding to the access structure 𝔸*) chosen by the adversary. Then, upon receiving the decryption query, the challenger *B* runs the algorithm *Designcryption* (*CT**, *PK*, SK_{Udi}) → *M* and returns *M* to *A* if it is a valid plaintext; otherwise, it outputs a "failure" message ⊥.

Challenge: The adversary *A* chooses two target plaintexts M_0 and M_1 and a signing set of attributes U_s which corresponds to an identity ID_{Us} and sends them to the challenger *B*. When receiving the target plaintexts and the private key SK_{Us}, *B* randomly chooses *b* from {0,1} and executes Signcryption (*PK*, M_b, SK_{Us}, 𝔸*, *c*). Then, the challenger sends *CT** to the adversary.

Query Phase 2: After receiving *CT** the adversary can perform a number of queries like Phase 1. Note that *A* cannot query the identity information S*= $\{ID_1{}^*, \ldots ID_n{}^*\}$ in the dExtract query and cannot query the ciphertext *CT** in the Designcryption query.

Guess: The adversary outputs his guess *b*' ∈ {0,1} and wins the IND- (H-CLSC)-CCA game if *b* = *b*'. The advantage of the adversary *A* in the above game is defined as:

$$\text{Adv}_{GSC}^{\text{IND}-(\text{H}-\text{CLSC})-\text{CCA}}(\text{A}) = \left|\Pr(b' = b) - \frac{1}{2}\right|$$

Unforgeability: The H-CLSC is signature-unforgeable against chosen policy and message attacks if the advantage of any probabilistic polynomial time (PPT) forger *F* is negligible in the game defined as follows:

Setup: The challenger *B* runs the Setup(1^λ) algorithm to generate master key *MK* that is kept secret and public parameters *PK* that are given to the forger *F*. Upon receiving the public parameters, *F* outputs multiple identities (corresponding to a DNF challenge access structure *A**) *S** = $\{ID_1{}^*, \ldots ID_n{}^*\}$.

Attack: The forger *F* can ask some queries to challenger *B* as follows:

- sExtract query: In this phase, *F* can adaptively ask for the signing private key. For the signer attribute set U_s, the challenger calls *sExtract* (*PK*, *MK*, U_s) → SK_{Us} and sends SK_{Us} to the adversary.
- dExtract query: Upon receiving the private key dExtract query about an attribute set U_{di} which corresponds to an identity ID_i, where $ID_i \neq ID_i{}^*$, i = 1, 2, …, *n*. The challenger runs the dExtract algorithm to get *dExtract* (*PK*, *MK*, U_{di}, *c*) → SK_{Udi}
- Signcryption query: *F* can ask for a signcryption on any message *M* and any access structure 𝔸 that is converted to a set of receivers' identities $S = \{ID_1, \ldots ID_n\}$. When receiving the query, the challenger runs *sExtract* (*PK*, *MK*, U_s) algorithm and gets the signing private key SK_{Us} as output. Then *B* computes the ciphertext *CT* = *Signcryption* (*PK*, *M*, SK_{Us}, 𝔸, *c*) and forwards *CT* to *F*.

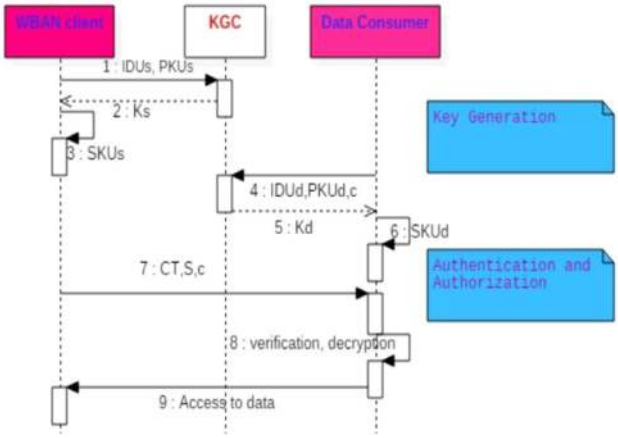

Fig. 3 – H-CLSC Authentication and Authorization scheme.

Forge: After the query phase, *F* outputs a ciphertext *CT** and a set of identities (corresponding to the challenge access structure 𝔸*) *S** = $\{ID_1{}^*, \ldots ID_n{}^*\}$. If *CT** can be decrypted correctly by every data consumer ID_i (having the set of attributes U_{di}) where i ∈ {1, 2…, *n*} in the set *S*, then the source of the sender is verified, *CT* is valid and *F* wins the game. The restriction here is that *F* cannot ask for the decryption private key of $ID_i{}^*$, and *CT** cannot be computed by the signcryption algorithm. The advantage of *F* is defined as the probability that he outputs a valid forgery.

5.3. *Proposed H-CLSC scheme*

The proposed H-CLSC scheme (presented in Fig. 3) consists of the following four phases.

5.3.1. *System initialization*

To initialize the system, this algorithm takes as input a secure parameter λ and performs the following steps:

- Let $\mathbb{G}_1$ be an additive group and $\mathbb{G}_2$ be a multiplicative group with the same prime order *q*. Then, the NM chooses randomly a generator *P* of $\mathbb{G}_1$ and constructs a bilinear pairings *e*: $\mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$
- Let $H_1 : \{0,1\}^* \rightarrow \mathbb{G}_1 H_2 : \mathbb{G}_2 \rightarrow \mathbb{Z}_q{}^*$, $H_3 : \{0,1\}^{|M|} \times \mathbb{Z}_q{}^* \times \cdots \times \mathbb{Z}_q{}^* \times \mathbb{G}_1 \rightarrow \mathbb{G}_1$, H_4: $\mathbb{Z}_q{}^* \rightarrow \{0,1\}^w$ and H_5: $\{0,1\}^w \rightarrow$

$\{0,1\}^{|M|}$ be five secure hash functions, where $|M|$ is the length of the plaintext message and w is a random integer

- The NM randomly selects a master key $MK \in \mathbb{Z}_q^*$ and computes the corresponding public key $P_{pub} = MK.P$
- It keeps the master key MK secret and publishes the system parameters PK given by:

$$PK = \{\mathbb{G}_1, \mathbb{G}_2, q, e, P, P_{pub}, H_1, H_2, H_3, H_4, H_5\}$$

5.3.2. *Key generation*

This algorithm presents the interaction between the WBAN client/data consumer and the NM. Based on the contextual information c and the set of attributes owned by the user, he proves his authorization and permissions to the NM. After verifying the authorization, the NM uses the master key MK, the public parameters PK, and the given attributes set U to generate a private key SK_U. In the proposed scheme, we employ two kinds of key generation algorithms as follows (to distinguish the role of signers and receivers, we define the signing key as SK_{Us} and the decryption key as SK_{Ud}):

(a) sExtract (PK, MK, U_s): Given the public parameters PK, the master key MK, and the set of signing attributes U_s, this algorithm runs the following steps:
- A signer with a set of signing attribute set U_s that is converted on an identity ID_{Us} by exploiting the conversion between access structures and identities, generates a random number α_s and calculates the public key $PK_{Us} = \alpha_s P$. Then, he sends ID_{Us} to the NM
- The NM computes $Q_s = H_1(ID_{Us})$ and $K_s = MK.Q_s$
- The NM sends back $\{K_s\}$ through a secure channel to the signer who calculates $h = H_1(PK_{Us} \| ID_{Us})$ and his own signing key $SK_{Us} = K_s + \alpha_s h$

(b) dExtract (PK, MK, U_d, c): On receiving the key generation request from a data consumer with decryption attribute set U_d under a contextual information c that includes the domain label, the data type as well as the patient's condition, this algorithm performs the following steps:
- The receiver attribute set is converted to an identity ID_{Ud}, then the data consumer selects a random number α_d, calculates $PK_{Ud} = \alpha_d P$ and sends (ID_{Ud}, c) to the NM
- The NM calculates $Q_d = H_1(ID_{Ud})$ and $K_d = MK.Q_d$
- The NM sends through a secure channel $\{K_d\}$ back to the data consumer who computes $h_2 = H_1(PK_{Ud} \| ID_{Ud} \| c)$ and defines his own decryption key $SK_{Ud} = K_d + \alpha_d h_2$

5.3.3. *Signcryption phase*

The Signcryption phase is performed by the signer who defines an access structure $\mathbb{A}$ for a given contextual information c as follows:

- The access structure $\mathbb{A}$ is converted to a set of n receivers with identities $S = \{ID_1, \ldots ID_n\}$
- Choose a random number r and a bit string $\delta \in \{0,1\}^w$ and calculates $Y_i = rQ_{di}$, $U = rP$, $R_i = rh_{2i}$ where $Q_{di=} H_1(ID_i)$, $h_{2i} = H_1(PK_{Udi} \| ID_i \| c)$
- For $i = 1,2 \ldots n$, the signer computes $z_i = H_2(e(PK_{Udi}, R_i)\, e(P_{pub}, Y_i))$
- Choose a random $s \in \mathbb{Z}_q^*$ and define a polynomial $f(x)$ with degree n as follows:

$$f(x) = \prod_{i=1}^{n} (x - z_i) + s(mod q) = a_0 + a_1 x + \ldots + a_{n-1} x^{n-1} + x^n$$

- Compute $\vartheta = \delta \oplus H_4(s)$, $Z = E_{H5(\delta)}(M)$, $X = e(Q_s, U)$ and $L = H_3(X, U, Z, \vartheta, c, t_s, a_0, a_1, \ldots a_{n-1})$ and then calculate $V = rQs + L.SK_{Us}$, where SK_{Us} is the signing key and t_s denotes the current timestamp
- Generate the ciphertext: $CT = \langle U, Z, \vartheta, V, t_s, a_0, a_1, \ldots a_{n-1} \rangle$

5.3.4. *Designcryption phase*

Given the ciphertext CT, a receiver with an identity $ID_i \in S$ who possesses a set of authorized attributes executes the following steps to verify the signature and decrypt the ciphertext CT:

- Upon receiving $CT = \langle U, Z, \vartheta, V, t_s, a_0, a_1, \ldots a_{n-1} \rangle$, check the validity of t_s while verifying $|t_s - t| \leq \Delta t$ where Δt is the preset maximum transmission delay and t is the current time. Reject the message if it is not valid; otherwise,
- Compute $h = H_1(PK_{Us} \| ID_{Us})$ and $Q_s = H_1(ID_{Us})$.
- Compute $L = H_3(X, U, Z, \vartheta, c, t_s, a_0, a_1, \ldots a_{n-1})$
- Verification: If the equation $X = (e(h, PK_{Us})\, e(Q_s, P_{pub}))^{-L} e(V, P)$ holds, the ciphertext is valid. Otherwise, the ciphertext is rejected and the receiver drops the decryption process.
- Compute $z_i' = H_2(e(SK_{Udi}, U))$ and $s = f(z_i')$
- Compute $\delta = \vartheta \oplus H_4(s)$
- Recover the message: $M' = D_{H5(\delta)}(Z)$

Correctness of the verification

$$\begin{aligned} X &= e(V,P)\Big(e(h, PK_{Us})e\Big(Q_s, P_{pub}\Big)\Big)^{-L} \\ &= e(rQ_s + L.SK_{Us}, P)\Big(e(h, PK_{Us})e\Big(Q_s, P_{pub}\Big)\Big)^{-L} \\ &= e(rQ_s, P)e(L.SK_{Us}, P)(e(-L.h, \alpha_s P)e(-L.Q_s, MK.P)) \\ &= e(Q_s, U)e(L.SK_{Us}, P)(e(-\alpha_s L.h, P)e(-L.MK.Q_s, P)) \\ &= e(Q_s, U)e(L.SK_{Us}, P)(e(-L(\alpha_s.h + MK.Q_s), P) \\ &= e(Q_s, U) \end{aligned}$$

Correctness of the decryption

$$\begin{aligned} z'_i &= H_2(e(SK_{Udi}, U)) \\ &= H_2(e(K_{di} + \alpha_{di} h_{2i}, rP)) \\ &= H_2(e(MK.Q_{di}, rP)e(\alpha_{di} h_{2i}, rP)) \\ &= H_2(e(MK.Q_{di}, rP)e(\alpha_{di} h_{2i}, rP)) \\ &= H_2\Big(e\Big(P_{pub}, rQ_{di}\Big)e(PK_{Udi}, rh_{2i})\Big) \\ &= H_2\Big(e\Big(P_{pub}, Y_i\Big)e(PK_{Udi}, R_i)\Big) \\ &= z_i \end{aligned}$$

6. H-CLSC 's security and performance analysis

In this section, we evaluate the effectiveness and efficiency of the proposed scheme. At first, we conduct a security analysis to present the security functionalities ensured by the

proposed scheme. Then, we assess the compliance of the proposed scheme with the Health Insurance Portability and Accountability Act (HIPAA) privacy and security requirements. Finally, a comparative study of benchmarking approaches is performed to assess its security properties, communication overhead, storage overhead as well as computation cost.

6.1. *Security analysis*

- *Ciphertext authenticity and Public verification*: In the proposed scheme, any third party can verify the validity of the ciphertext $CT = \langle U, Z, \vartheta, V, t_s, a_0, a_1, \ldots a_{n-1} \rangle$ without any information about the message M or the private key of the receiver. In fact, for a given public parameters *PK*, a sender identity ID_{Us} (corresponding to the signer set of attributes U_s), a signer public key PK_{Us}, anyone can verify the signer's signature and compute $h = H_1(PK_{Us} \| ID_{Us})$, $Q_s = H_1(ID_{Us})$ and $e(V, P) = (e(h, PK_{Us}) * e(Q_s, P_{pub}))^{L} * e(Q_s, U)$. If the ciphertext isn't valid, the receiver can reject the ciphertext without decrypting it.
- *Context-aware privacy*: In order to provide contextual privacy, the proposed scheme implies the contextual information to determine who can access what and under which context. In fact, each access structure is defined on the basis of the dynamic context changes which includes the patient's condition severity, the data type, the data consumer roles and their domains (PUD/PSD). Under such construction, the right access is permitted to the right party.
- *Anonymity and untractability*: During the authentication and authorization process, the WBAN client can sign a message using a set of signing attributes satisfying a given signing policy. In such an assumption, a signature reveals nothing about the identity of the signer beyond what is explicitly revealed by the attribute-based authentication policy. Under this notion, different signatures cannot be identified as sent by the same WBAN and we can assume that the signer is an authorized user. Therefore, unauthorized data consumers and adversaries cannot disclose who is the WBAN client or assign the multiple authentication sessions to the same patient (trace the patient's action).
- *Impersonation attack by KGC and escrow problem*: The key escrow problem can be solved in the proposed scheme such that the NM cannot impersonate the WBAN client or the data consumer without being detected. In fact, either the WBAN client or the data consumer can generate his private key by himself and these keys cannot be accessed by the NM. Thus, the NM cannot decrypt messages or impersonate the WBAN client/the data consumer.
- *Replay attack*: To avoid the replay attack defined as the reception of previously delivered messages, the ciphertext involves the timestamp. Upon receiving the signcrypted message, the data consumer will check the freshness of the timestamp t_s before executing the other steps of the designcryption process. In this case, the data consumer could detect the replay attack easily.
- *Modification attack*: In order to disclose any unauthorized modification of the patient's health information, the WBAN client should use his private key to sign the message on the basis of a predefined access structure. Upon receiving the data, a data consumer could detect any modification by checking the validity of the signature without disclosing the real identity of the signer.
- *Security against chosen plaintext attacks*: In the following, we present the security proof of the proposed H-CLSC scheme in the random oracle model on the basis of a selective-ID game in Pang et al. (2015) and Li et al. (2016). In fact, we will only prove that the IBBSC can satisfy confidentiality and unforgeability given that it has been demonstrated in Fan et al. (2017) and Herranz (2017) that if an IBBSC scheme is secure, then the conversion from a CP-ABSC to an IBBSC is secure.

Theorem 1. *A Hybrid Certificateless Signcryption (H-CLSC) scheme is said to be indistinguishable against chosen ciphertext attacks (IND-(H-CLSC)-CCA) if no probabilistic polynomial time (PPT) adversary A has a non-negligible advantage in winning the IND-(H-CLSC)-CCA game under the DBDH assumption.*

Proof 1. We construct a challenger *B* that interacts with an adversary *A* to solve the instance of DBDH while computing $e(P, P)^{abc}$ from an instance (P, aP, bP, cP) of the DBDH problem. We consider five oracles H_1, H_2, H_3, H_4 and H_5 to simulate the system for *B*. The adversary *A* can queries PPT times to the oracles. *B* runs each phase of the IND-HCLSC-CCA game as follows:

Setup: The challenger *B* executes the setup algorithm. It sets $P_{pub} = aP$ and sends the public parameters $PK = \{G_1, G_2, q, e, P, P_{pub}, H_1, H_2, H_3, H_4, H_5\}$ to the adversary *A*. Upon receiving the parameters, *A* outputs the target multiple identities $S^* = \{ID_1^*, \ldots ID_n^*\}$ that correspond to the challenge access structure $\mathbb{A}^*$.

Phase 1: *A* can request a number of queries. For the adversary *A* 's hash queries q_{Hi}, the challenger uses H_i-*list* to record the results of hash functions H_i, $i = 1 \ldots 5$.

H_1-*Queries:* *A* asks a polynomial bounded number of H_1-queries on identities of his choice. At the *j*th- H_1-query, if $ID_j \neq ID_i^*$, *B* chooses $l_j \in \mathbb{Z}_q$ randomly, calculates $Q_j = H_1(ID_j) = l_j P$ and puts (ID_j, l_j, Q_j) in H_1-*list*. Then, *B* returns Q_j.

- *Extract partial private key:* When *A* asks a partial private key extract query on identity ID_j,

  If $ID_j = ID_i^*$, then *B* fails and aborts
  If $ID_j \neq ID_i^*$, then the list H_1-*list* may contain (ID_j, l_j, Q_j). *B* returns the partial private key $K_j = l_j aP$

- *Request public key*: When *A* asks a public key extract query on identity ID_j, *B* checks the *public key-list* which is initially empty. If there is a tuple $(ID_j, PK_{Uj}, \alpha_j)$, then *B* returns PK_{Uj}. Otherwise, *B* generates a new key pair, updates the *public key-list* and returns the public key.
- *Replace public key:* When *B* receives a replace public key query (ID_j, PK_{Uj}), *B* first finds $(ID_j, PK_{Uj}, \alpha_j)$ on *public key-list*, then, it updates *public key-list* with tuple $(ID_j, PK_{Uj}, \perp)$.
- *sExtract private key:* When *A* asks a signing private key extract query on identity ID_j, if *B* replaces the public key of ID_j, then return $\perp$; otherwise, *B* finds in *public key-list* $(ID_j, PK_{Uj}, \alpha_j)$ and returns α_j.
- *dExtract private key*: When *A* asks a decryption private key extract query on identity ID_j and under a contextual information *c*, if *B* replaces the public key of ID_j, then return $\perp$;

otherwise, B finds in *public key-list* (ID_j, PK_{Uj}, c, α_j) and returns α_j.

H_2-Query: The challenger B determines if (P, Q_i, P_{pub}, U, W_j) uses DBDH oracle for $i \in [1, q_{H2}]$ when he is queried with $W_j \in \mathbb{G}_2$ for some $j \in [1, q_{H2}]$ and $D \in \mathbb{G}_2$. If it exists, B should terminate the game for $e(P, P)^{abc}$. $D = W_j^{l_i^{-1}}$. Otherwise, B chooses a random number $x_j \in \mathbb{Z}_q{}^*$ and puts a tuple (W_j, x_j) into the H_2-*list*. Then, B returns x_j to the adversary A.

H_3-Query: Upon receiving the tuple (X_j, U_j, Z_j, ϑ_j, c, t_s, a_{j0}…, $a_{jn\text{-}1}$) where $j \in [1, q_{H3}]$, B picks randomly a value $L_j \in \mathbb{Z}_q{}^*$ and puts the tuple (X_j, U_j, Z_j, ϑ_j, c, t_s, a_{j0}…, $a_{jn\text{-}1}$, L_j) into the H_3-*list*. Then, B returns L_j.

H_4-Query: As an integer s_j is sent to the H_4 oracle where $j \in [1, q_{H4}]$, B chooses a random string $w_j \in \{0,1\}^w$ and puts (s_j, w_j) into the H_4-*list*. Then, the string w_j is sent to the adversary A.

H_5-Query: When A asks for the string $\delta_j \in \{0,1\}^w$ for $j \in [1, q_{H5}]$, B picks a random string $p_j \in \{0,1\}^{|M|}$ and puts the tuple (δ_j, p_j) into the H_5-*list*. Then, B returns p_j to the adversary A.

Key Generation query

- *sExtract query:* For a signing key extract query on ID_{Us} (corresponding to a set of signing attributes U_s), if $ID_{Us} \neq ID_i{}^*$, B searches for (ID_{Us}, PK_{Us}, α_s) in H_1-*list* and computes his signing private key $SK_{Us} = \alpha_s h + aQ_s$, where $h = H_1(PK_{Us} \| ID_{Us})$. Otherwise, B stops and outputs failure.
- *dExtract query:* Upon receiving a decryption key extract query on ID_{dj},
  if $ID_{dj} \neq ID_i{}^*$, B searches for (ID_{dj}, PK_{Udj}, α_{dj}, c) in H_1-*list* and computes his decryption private key $SK_{Udj} = \alpha_{dj}$ $H_1(PK_{Udj} \| ID_{Udj} \| c) + aQ_{dj}$. if $ID_{dj} = ID_i{}^*$, B aborts and outputs $\perp$.

Signcryption query: When A asks for a signcryption query, B checks whether there exist $ID_{Us} \neq ID_i{}^*$. Then, he proceeds the signcryption algorithm and gets the signing private key from the *sExtract query*, $SK_{Us} = \alpha_s H_1(PK_{Us} \| ID_{Us}) + aQ_s$. Otherwise, B simulates the signcryption algorithm as follows:

(1) Randomly choose $r' \in \mathbb{Z}_q{}^*$ and compute $U = r'P$, $Y_i = r'Q_{di}$, $R_i = r'\, H_1(PK_{Udj} \| ID_{Udj} \| c)$
(2) For $i = 1 \ldots n$, compute $z_i = H_2(e\,(PK_{Udi}, R_i)\; e\,(P_{pub}, Y_i))$
(3) Select randomly positive integer $s \in Z_q{}^*$ and define a polynomial $f(x)$ with degree n as follows:

$$f(x) = \prod_{i=1}^{n} (x - z_i) + s \pmod q$$
$$= a_0 + a_1 x + \ldots + a_{n-1} x^{n-1} + x^n$$

(4) Compute $\vartheta = \delta \oplus H_4(s)$, $Z = E_{H5(\delta)}(M)$, $V = r'Qs + L.\, SK_{Us}$, $X = e\,(h, PK_{Us})\; e\,(Q_s, P_{pub}))^{-L}\; e\,(V, P)$ where $L = H_3(X, U, Z, \vartheta, c, t_s, a_0, a_1, \ldots a_{n-1})$
(5) Generate the ciphertext: $CT = \langle U, Z, \vartheta, V, t_s, a_0, a_1, \ldots a_{n-1} \rangle$

Designcryption query: When the adversary asks for a designcryption query, he sends (CT_j, $ID_i{}^*$) to B where $i \in \{1, 2 \ldots n\}$, $CT_j = \langle U_j, Z_j, \vartheta_j, V_j, t_s, a_{j0}, a_{j1}, \ldots a_{jn-1} \rangle$. Then, the challenger B runs the following steps:

(1) Check the list H_3-*list* to find the tuple (X_j, U_j, Z_j, ϑ_j, c, t_s, a_{j0}…, $a_{jn\text{-}1}$). If it was found, B gets (Z_j, ϑ_j). Otherwise, the challenger B aborts and returns failure.
(2) Construct the polynomial $f(x) = a_{j0} + a_{j1}x + \ldots + a_{jn-1}x^{n-1} + x^n$
(3) Search the tuple (ID_j, l_j, Q_j) in the list H_1-*list*.
(4) For $l = 1 \ldots q_{H2}$, execute the following steps:
   (a) Search the tuple (W_l, x_l) from the list H_2-*list*.
   (b) Judge whether (P, Q_i, P_{pub}, U_j, W_l) uses the DBDH oracle by verifying the equation $e(P, P)^{ar'l_i} = W_l$. If it is the case, compute $s_l = f(x_l)$, $\vartheta_j = \delta_j{}' \oplus H_4(s_i)$ and $M_j = D_{H5(\delta j)'}\,(Z_j)$
(5) Verify if the equation $X_j = (e(h,\ PK_{Us})e\ (Q_s,\ P_{pub}))^{-L_j} e(V_j,\ P)$ holds, where $L_j = (X_j, U_j, Z_j, \vartheta_j, c, t_s, a_{j0} \ldots, a_{jn\text{-}1})$. If it holds, then get the plaintext M_j.
(6) Otherwise, B sends "failure" to A, which indicates that the ciphertext generated by the proposed scheme is invalid.

Challenge: The adversary A outputs a target plaintext pair (M_0, M_1) and an arbitrary signing private key SK_{Us} to the challenger B. B randomly chooses $\beta \in \{0,1\}$and signcrypts the message M_β. Then, the target ciphertext $CT^* = \langle U, Z, \vartheta, V, t_s, a_0, a_1, \ldots a_{n-1} \rangle$ is generated and sent to the adversary A, where $U = r'P$, $Z = E_{H5(\delta)}(M)$, $\vartheta = \delta \oplus H_4(s)$ and $V = r'Qs + L.\, SK_{Us}$.

Phase 2: A performs new queries as Phase 1. Note that the adversary cannot query the information of ($ID_1{}^*$, …$ID_n{}^*$) in the key generation query and CT^* in the designcryption query.

Guess: The adversary A outputs its guess $\beta' \in \{0,1\}$. If $\beta' = \beta$, A needs to issue H_2 query on $\Psi = e(P_{pub}, Y_i).D = e(aP, r'l_iP).D = e(P, P)^{ar'l_i}.D = e(P,P)^{abc}.D$. Hence, e ($P$, P) ^{abc} can be extracted from H_2-*list*.

According to the above analysis, we can get the advantage of B as the following equation. For q_d times Designcryption query, the probability that B rejects the valid ciphertext is less than $nq_d/2^k$. So, if A wins the game, B's advantage is given by:

$$p_1 = \Pr(\beta' = \beta | signcryption(PK,\ M_\beta, SK^*_{Us},\ \mathbb{A}^*,\ c) = \varepsilon + \frac{1}{2} - \frac{nq_d}{2^k}$$

$$p_2 = \Pr(\beta' = m | \Psi \in \mathbb{G}_2) = \frac{1}{2},\ m = \{0, 1\}$$

$$\varepsilon' = \left| \Pr(B(aP,\ bP,\ cP, \Psi) = 1) - \Pr\left(B\left(aP,\ bP,\ cP, e(P, P)^{abc}\right) = 1\right) \right|$$
$$\geq \left| \varepsilon + \frac{1}{2} - \frac{nq_d}{2^k} - \frac{1}{2} \right|$$
$$\geq \varepsilon - \frac{nq_d}{2^k}$$

Theorem 2. *A Hybrid Certificateless Signcryption (H-CLSC) is signature-unforgeable against chosen policy and message attacks if the advantage of any probabilistic polynomial time (PPT) forger F is negligible in the SUF-(H-CLSC)-CMA game under the CDH assumption.*

Proof 2. We construct a challenger B that interacts with a forger F to solve the CDH problem while computing abP from an instance (P, aP, bP). We consider five oracles H_1, H_2, H_3, H_4 and H_5 to simulate the system for B. The forger F can query PPT times to the oracles. B executes and answers each phase of the SUF-HCLSC-CMA game as follows:

Setup: The challenger B sets $P_{pub} = aP$ and sends the system parameters $PK = \{G_1, G_2, q, e, P, P_{pub}, H_1, H_2, H_3, H_4, H_5, E_k, D_k\}$ to F. Upon receiving the parameters, F outputs the target multiple identities $S^* = \{ID_1{}^*, \ldots ID_n{}^*\}$ that correspond to the challenge access structure $\mathbb{A}^*$.

Attack: F adaptively performs polynomial bounded number of queries similar to those in Phase 1 of Theorem 1.

Forgery: The forger F generates a tuple $(CT^*, ID_{Us}{}^*, L^*, PK_{Us}{}^*)$. If $ID_{Us} = ID_i{}^*$, $i = 1 \ldots n$, B aborts. Otherwise, B chooses different hash function $L'^*$and interacts with F through the same random tape, then the attacker can output a different forger $\langle CT'^*, L'^* \rangle$. According to the above analysis, both $CT^*$and CT'^* should satisfy the public verifiability condition.

$$X = \left(e(h, PK_{Us}{}^*)e\left(Q_s, P_{pub}\right)\right)^{-L^*} e(V^*, P)$$
$$X = \left(e(h, PK_{Us}{}^*)e\left(Q_s, P_{pub}\right)\right)^{-L'^*} e(V'^*, P)$$

Where $h = H_1(PK_{Us} \| ID_{Us}) = \beta P$ $Q_s = H_1(ID_{Us}{}^*) = bP$. B can compute: $abP = (V^* - V'^*)\ (L^* - L'^*)^{-1} - \beta PK_{Us}$ as the solution of the CDH problem. Therefore, B solves the CDH problem successfully. Hence, we estimate the advantage of forger's success in solving CDH problem. For q_s queries to the signcryption query, the probability that B fails is less than $q_s/2^k$ and the probability that B aborts when F makes a partial private key extraction is at most $1/q_{ppk}$, where q_{ppk} is the partial private key extract query. Consequently, if the forger F wins the game, the challenger B's advantage is:

$$\varepsilon' \geq \left(\varepsilon - \frac{q_s}{2^k}\right)\left(1 - \frac{1}{q_{ppk}}\right)^{q_{ppk}}$$

6.2. *Compliance with HIPAA regulations*

In this subsection, we discuss the compliance of the proposed H-CLSC scheme with the HIPAA privacy and security regulations. HIPAA aims to standardize security and privacy mechanisms for patient health information. According to HIPAA, a secure remote patient monitoring system should satisfy the following requirements: Patient's understanding, confidentiality, patient's control, data integrity, and consent exception (Wei-Bin and Chien-Ding, 2008).

6.2.1. *Patient's understanding*

The HIPAA requires that the patient has the right to understand and agree on how his data is used and kept. The digital signature mechanism can protect this right. In the proposed scheme, the WBAN client uses his private key to sign the message. Thus, the signed ciphertext ensures that the WBAN client cannot deny his responsibility for the sent message.

6.2.2. *Confidentiality*

To guarantee confidentiality, the patient health information is encrypted using H-CLSC and only data consumers who satisfy the access structure can access data. Specifically, the confidentiality of the proposed H-CLSC scheme is proved through formal security analysis (Theorem 1).

6.2.3. *Patient's control*

In the proposed H-CLSC scheme, the WBAN client has the right to restrict access of any designated data consumer to his data. In fact, he defines who can access what and under which context. Hence, by controlling his access structure, the patient can control access to his data.

6.2.4. *Data integrity*

In the proposed H-CLSC scheme, the ciphertext is signed, thus, any change in the message will invalidate the signature. Furthermore, there is no efficient way to modify an encrypted message and its signature to produce a new message with a valid signature. Upon receiving the ciphertext, a data consumer could detect any modification by checking the validity of the signature.

6.2.5. *Consent exception*

The use and disclosure of the patient data without the patient's permission is authorized in an emergency situation for life-saving purposes. In fact, in such situations, a data consumer can gain temporary access while contacting the NM that manages his identity and the emergency key. After the emergency is over, the patient can revoke the emergent access.

6.3. *Performance analysis*

In this section, we conduct a quantitative analysis to assess the security properties of the proposed scheme and evaluate its performance characteristics. In fact, H-CLSC scheme is compared with the LRSA (Zhang et al., 2017), R-CLE/S (Hu and Qin, 2015), and CP-ABE (Hu et al., 2016) schemes in terms of security properties, storage overhead, communication overhead as well as computation cost. In addition, the security properties of the proposed scheme are assessed according to the HPKI scheme (Jiankun et al., 2010) that verifies the HIPAA requirements. We shall notice that the benchmarking schemes apply different methods to design the authentication and authorization model. As a first step, we will only consider the communication between one data owner and one data consumer to perform the comparison between the different schemes. As a second step, we will study the impact of the number of data consumers on the communication overhead. Only the resource-constrained devices (controller/sensor nodes) are considered. In the following evaluation, the bilinear e employs the Tate pairing. The elliptic curve is defined over F_p. The order q of $\mathbb{G}_1$ and $\mathbb{G}_2$ is a 20-byte prime. In order to guarantee 80-bit security level, p should be a 64-byte prime if $\mathbb{G}_2$ is a q-order subgroup of the multiplicative group of the finite field $F_{p2}{}^*$. Based on the assumption used in (Hu et al., 2016), we can set p to be 42.5 bytes in length for the finite field $F_{p3}{}^*$. The length of an element in group $\mathbb{G}_1$ is 1024 bits using an elliptic curve with $q = 160$ bits. According to the standard compression method (Li et al., 2017; Ferrara et al., 2015), the size of an element in group $\mathbb{G}_1$ can be compressed to 65 bytes (Table 1).

6.3.1. *Security properties*

In this subsection, we evaluate the functional security of the proposed scheme while comparing the security properties of the H-CLSC model with the different benchmark schemes in Table 2. The capacity of the security and privacy preserving scheme is expressed in terms of confidentiality, integrity, anonymity, ciphertext authenticity, public verification, context-aware privacy, certificateless, untraceability, key escrow resilience and resistance against attacks.

Table 1 – Notation used in the proposed H-CLSC scheme.

Notation	Description
q	A prime number
$\mathbb{G}_1$	An additive group with order q
$\mathbb{G}_2$	A multiplicative group with order q
e	A bilinear pairing
P	A generator of the group $\mathbb{G}_1$
H_1 H_2 H_3 H_4 H_5	One-way hash functions
PK, MK	System public key and master key
PK_{Ui}	The public key of user i
SK_{Ui}	The secret key of user i
U	The universe of attributes
U_i	The attributes set of user i
$\mathbb{A}$	An access structure
c	Patient's contextual information {user's domain, data type, patient's status}
t_s	The current timestamp of the WBAN client
$E_k()$, $D_k()$	The symmetric encryption and decryption where k is the key.

Table 2 – Overall comparison of security properties.

Scheme	LRSA	R-CLE/S	CP-ABE	H-CLSC	HPKI
Confidentiality	+	+	+	+	+
Integrity	+	+	+	+	+
Anonymity	+	+	+	+	−
Ciph.Auth	−	−	−	+	+
Pub.Verif	−	−	−	+	+
Context-privacy	−	−	−	+	−
No.Certificate	+	+	−	+	−
Untraceability	+	+	+	+	−
No. Key escrow	+	+	−	+	+
Attack.Resistance	−	−	−	+	−

Table 3 – Storage overhead comparison.

Scheme	WBAN client's storage overhead
LRSA	$\|\mathbb{G}_1\|+\|Z_q^*\| = 85$ bytes
R-CLE/S	$2^*\|\mathbb{G}_1\|+\|Z_q^*\| = 150$ bytes
CP-ABE	$N^*\|\mathbb{G}_1\|+\|Z_q^*\| = 65^*N+20$ bytes
H-CLSC	$\|\mathbb{G}_1\| = 65$ bytes

6.3.2. *Storage overhead*

The storage overhead is an expressive metric of any authentication and access control scheme because both the client and the data consumer should store the secret keys for Signcryption/Designcryption. In the H-CLSC scheme, the WBAN client and the data consumer need to store $\{SK_{Ui}\}$, where SK_{Ui} is an element of $\mathbb{G}_1$. Therefore, the users' storage overhead is 65 bytes. As presented in Table 3, the WBAN client in the proposed scheme requires less storage overhead than the other schemes (Zhang et al., 2017; Hu et al., 2016; Hu and Qin, 2015).

As shown in Fig. 4, for the CP-ABE scheme, the storage overhead increases with the number of attributes. However, in the H-CLSC scheme, the storage overhead is independent of the number of attributes and it has a fixed size.

6.3.3. *Communication overhead*

The encrypted data should be stored in the controller and transmitted to the data consumers when requested. In this

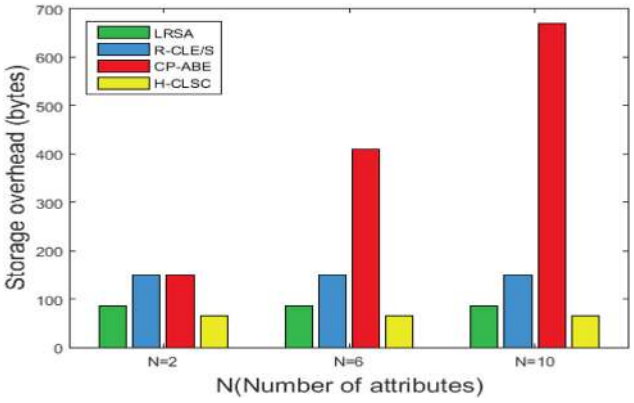

Fig. 4 – Storage overhead vs. number of attributes.

Table 4 – Communication overhead comparison.

Scheme	Controller (bytes)	Sensor node(bytes)
LRSA	$4\|\mathbb{G}_1\|+6\|Z_q^*\|+2\|ID\|+\|M\| = 420$	–
R-CLE/S	$\|\mathbb{G}_1\|+8^*\|Z_q^*\|+\|M\|+\|ID\| = 255$	–
CP-ABE	$5\|\mathbb{G}_2\|+ 24 = 236.5$	$10\|\mathbb{G}_2\|+76 = 501$
H-CLSC	$2\|\mathbb{G}_1\|+\|Z_q^*\|+\|M\|+w = 180$	–

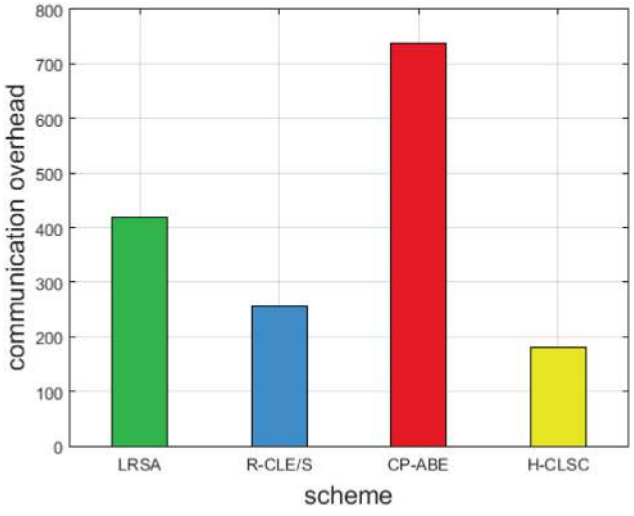

Fig. 5 – Communication overhead comparison.

context, the communication overhead is mainly associated with the size of the ciphertext. In the proposed scheme, the ciphertext size dependent on the number of consumers. Firstly, as shown in Table 4 and Fig. 5, we considered only one data consumer and conducted comparisons in terms of communication overhead between the four schemes. In the proposed H-CLSC scheme, the WBAN client needs to transmit: $2|\mathbb{G}_1| + n|Z_q^*| + |M| + w$, where w is the bit length of a string and we assume that $w = 10$ bytes and n is the number of data consumers.

Fig. 6 illustrates the impact of the number of data consumers on the communication overhead which increases linearly with the number of data consumers. The proposed

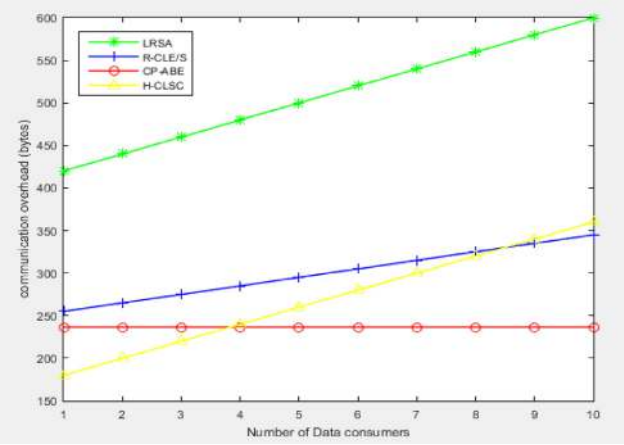

Fig. 6 – Communication overhead vs. number of data consumers.

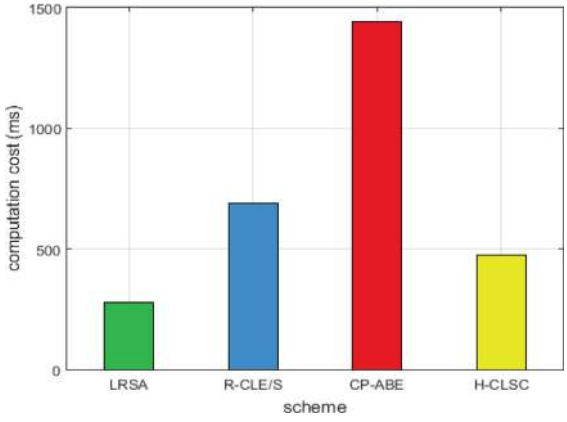

Fig. 7 – Computational cost comparison.

Table 5 – Computation cost comparison.

Scheme	Controller (ms)	Sensor node(ms)
LRSA	$9T_M = 276.03$	–
R-CLE/S	$11T_E+T_P = 688.5$	–
CP-ABE	$5T_P = 481$	$10T_P = 962$
H-CLSC	$3T_P+6T_M = 472.62$	–

scheme has significantly lower communication overhead than the LRSA scheme and an acceptable communication cost compared to the R-CLE/s scheme.

6.3.4. *Computation cost*

In this subsection, we compare the proposed H-CLSC scheme with the benchmarking models in terms of computational cost. As the operations on pairing, exponentiation, and multiplication heavily affect the computational overhead, we only consider these three operations. We denote T_E the time consumed for one exponentiation operation, T_M the time consumed for one scalar multiplication in $\mathbb{G}_1$, and T_P the time for one pairing operation.

In the H-CLCS scheme, the signcryption process in WBAN client takes six multiplication operations in $\mathbb{G}_1$ and three pairing operations in $\mathbb{G}_2$. The computational cost for the H-CLCS scheme and the other authentication and authorization models are presented in Table 5. According to Zhang et al. (2017), to quantify the running time of the operations, the algorithms are implemented on an Intel PXA270 processor at 624 MHz installed on the Linux personal digital assistant. The running time of the different operation are $T_E = 53.85$ ms, $T_M = 30.67$ ms, and $T_P = 96.20$ ms, respectively.

As shown in Fig. 7, the proposed H-CLSC scheme has the more computational cost compared to the LRSA scheme but achieves better performance compared to CP-ABE and R-CLE/S schemes.

Finally, we can notice that the proposed H-CLSC scheme achieves better performances when we employ the MNT curve of embedding degree $k = 6$, $q = 160$ bits and a field size of $\mathbb{G}_1$=160 bits (Lu et al., 2012; Ruj and Nayak, 2013).

7. Conclusion

In this paper, we have proposed a novel efficient Hybrid Certificateless Signcryption (H-CLSC) scheme that combines the features of CP-ABSC and IBBSC to provide context-aware access control and anonymous authentication. Security analysis proved the effectiveness of the proposed scheme that can satisfy confidentiality, integrity, anonymity, context-aware privacy, untraceability, ciphertext authenticity, and public verifiability. Furthermore, the key escrow problem is solved through our model while using certificateless signcryption. Performance analysis demonstrated the efficiency of the H-CLSC scheme that has lower storage and communication overhead than the benchmarking schemes. In addition, the proposed scheme ensures a desired computational cost compared to the other schemes.

Conflict of Interest

All authors have participated in (a) conception and design, or analysis and interpretation of the data; (b) drafting the article or revising it critically for important intellectual content; and (c) approval of the final version.

This manuscript has not been submitted to, nor is under review at, another journal or other publishing venue.

The authors have no affiliation with any organization with a direct or indirect financial interest in the subject matter discussed in the manuscript.

REFERENCES

Aziz SM, Pham DM. Energy efficient image transmission in wireless multimedia sensor networks. IEEE Commun Lett 2013;17:1084–7. doi:10.1109/LCOMM.2013.050313.121933.

Fan C-I, Tseng Y-F, Lin C-W. Attribute-Based Encryption from Identity-Based Encryption. IACR Cryptography ePrint Archive 2017 2017.

Ferrara AL, Green M, Hohenberger S, Pedersen MØ. Practical Short Signature Batch Verification. IACR Cryptography ePrint Archive 2008 Report 2008/015.

Herranz J. Attribute-based encryption implies identity-based encryption. IET Inf Secur 2017.
He D, Zeadally S, Kumar N, Lee JH. Anonymous authentication for wireless body area networks with provable security. IEEE Syst J 2016:1–12.
Huawei Z, J Qin, Jiankun H. An energy efficient key management scheme for body sensor networks. IEEE Trans Parallel Distrib Syst 2013;24:2202–10.
Hu C, Li H, Huo Y, Xiang T, Liao X. Secure and efficient data communication protocol for wireless body area networks. IEEE Trans Multi-Scale Comput Syst 2016;2(2).
Hu J, Chen H-H, Hou T-W. A hybrid public key infrastructure solution (HPKI) for HIPAA privacy/security regulations. Comput. Stand. Interfaces Arch. 2010;32(5-6):274–80.
Hu X, Qin Z. Revocable and scalable certificateless remote authentication protocol with anonymity for wireless body area networks. IEEE Trans Inf Forensics Secur 2015;10(7):1442–55.
Javadi SS, Razzaque MA. Security and privacy in wireless body area networks for health care applications. Wirel Netw Secur 2013:165–87.
Pham DM, Aziz SM. Object extraction scheme and protocol for energy efficient image communication over wireless sensor networks. Comput Netw 2013;57:2949–60 2013. doi:10.1016/j.comnet.2013.07.001.
Lai J, Deng RH, Guan C, Weng J. Attribute-based encryption with verifiable outsourced decryption. IEEE Trans Inf. Forensics Secur 2013;8(8):1343–54.
Lee W-B, Lee C-D. A cryptographic key management solution for HIPAA privacy/security regulations. IEEE Trans Inf Technol Biomed 2008;12(1).
Li F, Liu Bo, Hong J. An efficient signcryption for data access control in cloud computing. Comput. J. 2017.
Li M, Yu S, Lou W, Ren K. Group device pairing based secure sensor association and key management for body area networks. In: Proceedings of the IEEE INFOCOM; 2010. p. 1–9.
Li M, Yu S, Guttman J, Lou W, Ren K. Secure ad hoc trust initialization and key management in wireless body area networks. ACM Trans Sensor Netw 2013;9(2):1–35 Article ID: 18.
Li M, Yu S, Zheng Y, Ren K, Lou W. Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption. IEEE Trans Parallel Distrib Syst 2013;24(1):131–43.
Li Y, Wang C, Zhang Y, Niu S. Privacy-preserving multi-receiver signcryption scheme for heterogeneous systems. Secur Commun Netw 2016;9(17).
Liu J, Zhang Z, Chen X, Kwak KS. Certificateless remote anonymous authentication schemes for wireless body area networks. IEEE Trans Parallel Distrib Syst 2014;25(2): 332–342.
Liu J, Zhang L, Sun R. 1-RAAP: an efficient 1-round anonymous authentication protocol for wireless body area networks. Sensors 2016;16:728. doi:10.3390/s16050728.
Liu J, Li Q, Yan R, Sun R. Efficient authenticated key exchange protocols for wireless body area networks. EURASIP J Wirel Commun Netw 2015.
Lu R, Lin X, Shen X. SPOC: a secure and privacy-preserving opportunistic computing framework for mobile-healthcare emergency. IEEE Trans Parallel Distrib Syst 2013;24(3):614–24.
Lu R, Liang X, Li X, Lin X, Shen X. EPPA: an efficient and privacy-preserving aggregation scheme for secure smart grid communications. IEEE Trans Parallel Distrib Syst 2012;23(9).
Malasri K, Wang L. Design and implementation of a secure wireless mote-based medical sensor network. Sensors 2009;9(8):6273–97.
Mao X, Lai J, Mei Q, Chen K, Weng J. Generic and efficient construction of attribute-based encryption with verifiable outsourced decryption. IEEE Trans Depend Secure Comput 2016;13(5):1–14.
Pang L, Gao L, Li H, Wang Y. Anonymous multi-receiver ID-based signcryption scheme. IET Inf Secur 2015;9(3):194–201.
Ruj S, Nayak A. A decentralized security framework for data aggregation and access control in smart grids. IEEE Trans Smart Grid 2013;4(1).
Sahai A, Waters B. Fuzzy identity-based encryption. In: LNCS, 3494; 2005. p. 457–73.
Samaneh M, Mehran A, Justin L, David S, Abbas J. Wireless body area networks: a survey. IEEE Commun Surv Tuts 2014;16(3):1658–86.
Tan CC, Wang H, Zhong S, Li Q. IBE-lite: a lightweight identity-based cryptography for body sensor networks. IEEE Trans Inf Technol Biomed 2009;13(6):926–32.
Xiong H. Cost-effective scalable and anonymous certificateless remote authentication protocol. IEEE Trans Inf Forensics Secur 2014;9(12):2327–39.
Zhang A, Wang L, Ye X, Lin X. Light-weight and robust security-aware D2D-assist data transmission protocol for mobile-health systems. IEEE Trans Inf Forensics Secur 2017:662–75.
Zhao H, Chen C, Hu J. Securing body sensor networks with biometric methods: a new key negotiation method and a key sampling method for linear interpolation encryption. Int J Distrib Sensor Netw 2015.
Zhibo P. Technologies and architectures of the internet-of-things (IoT) for health and well-being M.S. thesis. Stockholm, Sweden: Deptartment of Electronic and Computer Systems, KTH-Royal Institute of Technology; 2013.